Checklist:
Critical Security Changes

Starting Exercise

□ **List out 5 of your most important online accounts.** These are accounts which, if hacked, could cause irreparable damage or harm to you.

1. ______________________________
2. ______________________________
3. ______________________________
4. ______________________________
5. ______________________________

Recommended accounts: banks, investment accounts, email, Paypal, Facebook, etc.

□ **Rate the strength of your current password.** Use this password strength checker tool to determine if your passwords are strong.

My primary password was rated as: ______________________________

**Note: For security's sake, do not input your actual password in any password checker tool. Instead, type something similar to your password, perhaps changing some numbers or letters.*

□ **List your top social media accounts.** It doesn't matter if you don't post on them regularly, it's important to take inventory of which social profiles you have.

1. ______________________________
2. ______________________________
3. ______________________________
4. ______________________________
5. ______________________________

Keep this exercise handy as you complete the rest of this checklist!

Examples include: Facebook, Instagram, WhatsApp, Twitter, TikTok, etc.

Immediate Security Changes (<1 hour)

□ **Change the passwords of all your top 5 important online accounts.**

Even if your password strength was rated as "Very Strong", it still might be a good idea to change your passwords here. Ask yourself these questions:

- Do I use the same password on multiple accounts?
- Have I had this same password for years?
- Have I ever shared this password anywhere?

If the answer to any of the above questions was "yes", you should go in and change your password for these accounts. There are many ways to create a strong password. For example, you could:

- Come up with your own password strategy (see this video for ideas)
- Use a password generator
- Start using a password manager app (I recommend 1Password)

□ **Install an Authenticator App for 2-Factor Authentication (2FA)**

There are a number of free authenticator apps that you could download on your phone or tablet. They all perform the same function, but each has its own strengths and weaknesses. I recommend:

- 1Password (paid)
- Authy (free)
- Google Authenticator (free)

After the app is installed, log in and turn on 2FA for each of your five most important accounts (if possible). Here are a few resources to help you do this:

- Which accounts allow for 2FA?
- How to set up 2FA (tutorial)

□ Lock & Track your Mobile Devices

What would happen if your mobile device were lost or stolen? It happens more often than you think. Here are three things you can easily do to secure your device:

1. **Set a passcode lock** (use at least 6 digits, not 4!)
2. **Enable "Find My Phone" or "Locate My Phone."** This will allow you to track a device that has been lost or stolen.
3. **Update Your Medical ID info.** While this information can be useful should you have a health emergency, you can also set it to be accessible from the lock screen so that a good Samaritan who finds your phone can contact you to return it.

□ Double-Check Your Home Network

As our homes fill with Internet of Things (IoT) devices, your home network has become a critical component of your overall security. Unauthorized access to your home network could allow somebody easy access to your home security system, your video surveillance system, your computers and more.

To ensure maximum security for your home network, follow these steps:

- **Change Your Router Password:** Most of us use the password that came with our router. While this password is usually secure, it's also often printed on the side of your router and visible to anybody who comes into your home, such as neighbors, maintenance workers, and cleaners.
- **Create a Guest Network:** Most routers allow you to create a secure guest network so that you don't have to give out the password and access to your primary home network. Use this if you have it!
- **Turn Off Remote Access:** Remote access is a network vulnerability that for some reason is defaulted to "on" for most routers. Unless you have a specific reason to need someone to access your network remotely, turn this off.

To learn how to make all of these changes, be sure to check the All Things Secured Home Network Tutorial.

□ Make Your Social Media Private

We publish an alarming amount of personal information on our public social media profiles. It takes very little effort to change these privacy settings, and here's what is recommended

- **Instagram:** Unless you're a public figure, go into settings and turn on "Private Account".
- **Facebook:** A full privacy audit is advisable, but if you only do two things, make sure to "Limit Past Post Permissions" and change your profile information permissions. See how to do all this with our Facebook Privacy Tutorial.
- **LinkedIn:** Your contact email address should be a work email address that isn't used for any of your banking or investment accounts.
- **All Other Accounts:** View your profile and make sure you're comfortable with all of the information that is available publicly.

Advanced Privacy & Security

If you've completed the security changes listed above, the following are next steps you can take that will make a significant difference in your security and privacy online.

□ Start Using a Password Manager App

A password manager app is a piece of software that helps you create strong passwords, store them in an encrypted, digital vault and retrieve them easily. You get strong, unique passwords while only having to remember a single "master password". I recommend using 1Password.

Recommended:

1Password
Try free for 14 days

□ Freeze & Monitor Your Credit

The ability to easily open new lines of credit may be convenient, but it probably isn't in your best interest (for security and for financial reasons!). There are two common solutions that will give you more control over your credit and how it gets used:

Recommended:

IdentityForce
Try free for 14 days

- **Credit Freeze:** You can order a credit freeze with each of the three credit bureaus that locks your credit with PIN that only you know. The downsides are that there might be a fee to activate/lift the freeze and it makes applying for new credit a bit of a hassle.
- **Credit Monitoring:** The alternative to freezing your credit is to closely monitor it. Companies like IdentityForce monitor both your personal information (i.e. social security info) as well as any credit pulls or weird charges.

□ Backup Your Devices

One of the fastest growing digital scams is something known as "ransomware". In most cases, users are tricked into clicking a link or downloading some software that locks up their computer until a ransom is paid to the hacker.

Even if you ignore the risk of ransomware, there's still the possibility that your computer or mobile device will be lost or stolen. Do you have all your data backed up somewhere?

For sensitive data, it's best to store it in three places: on your device, in "the cloud" and on a separate physical hard drive. Here's what I recommend:

- **Online Secure Storage:** Google Drive, Tresorit or Sync.com
- **External Hard Drive:** Western Digital My Book

□ Hide Your Home Address & Phone Number

Did you know that it's possible to obtain a second home address and phone number that will receive mail and accept phone calls? You no longer have to give over your personal information on every form you receive, plus, you can now check your mail and voicemail from your phone.

- **Get a 2nd Address:**

Recommended:

TravelingMailbox
Try free for 14 days

- **Get a 2nd Phone Number:**

Recommended:

Hushed
Try free for 14 days

Each of these options has an app you download on your phone that alerts you when you have a new piece of mail (they will open and scan it for you) or a new voicemail/text message.